p–ISSN: 2723 - 6609 e-ISSN: 2745-5254
Vol. 5, No. 3 March 2024 http://jist.publikasiindonesia.id/

Development of A Risk Management System To Reduce The Impact of Cyber Threats

Rafi Farizki, Frasciskus Antonius Alijoyo
STMIK LIKMI Bandung, Indonesia
Email: rafifarizki90@gmail.com, franciskus.antonius.alijoyo63@gmail.com

*Correspondence: rafifarizki90@gmail.com

Keywords:
management system, risk management, Impact of Cyber Threats

ABSTRACT

Cyber threats are one of the main issues in the digital era. Cyberattacks can result in financial, reputational and even operational disruption for organizations. In an effort to overcome this, organizations need to have an effective risk management system to identify, assess and manage cyber risks. The aim of this research is to determine the effectiveness of a risk management system that can help organizations reduce the impact of cyber threats. This study used qualitative research methods. The data collection technique in this research is literature study. The data that has been collected is then analyzed in three stages, namely data reduction, data presentation and drawing conclusions. The research results show that developing an effective risk management system is an important step for organizations in reducing the impact of cyber threats. A good risk management system can help organizations protect information assets, increase cyber resilience, and build customer trust.

Introduction

The widespread use of the internet has resulted in an increase in cyberattack incidents. According to The Global Cybersecurity Index (GCI) 2017 report issued by the International Telecommunication Union (ITU), the state of cybersecurity in Indonesia is experiencing a maturing stage and is included in the category of countries with a low level of cybersecurity (Sudarmadi & Runturambi, 2019). According to records from the National Cyber and Encryption Agency (BSSN), the number of cyber attack cases in Indonesia has reached 100 million until April 2022. Concerns about this threat prompted governments and electronic system operators (PSEs) to step up system protection efforts and response to cyberattacks. An important role is also played by the Personal Data Protection Law (PDP) in maintaining data sovereignty and security (Abdullah & Ikasari, 2023).

Cyberthreats can result in vulnerabilities in the security of systems in data centers, which in turn can cause systems to become malfunctioning and vulnerable to various risks. One of the main risks is data theft, where attackers can access sensitive or confidential information stored in the system, such as customer data or company financial information. Cyberthreats can also cause data alteration, where stored data can be

manipulated or altered by attackers, leading to loss of data integrity and inaccuracies in the information provided by the system. In addition, cyberspace can also be faced with threats such as viruses, piracy, Denial of Service (DoS) attacks, and Distributed Denial of Service (DDoS), which can disrupt or stop online services, resulting in significant operational and reputational losses for the agency (Benyamin, Mualim, & Duarte, 2023).

To overcome these challenges, organizations need to have an effective risk management system in place in dealing with cyber threats. This system aims to identify, assess, and manage risks related to information system security. The government, through Presidential Regulation Number 53 of 2017 concerning the State Cyber and Encryption Agency (BSSN) and its amendments to Presidential Regulation Number 133 of 2017, established BSSN which is tasked with implementing cyber security effectively and efficiently by coordinating, developing, and consolidating all elements related to national cyber security. BSSN developed the Indonesian Cyber Security Strategy as a guideline for all national cybersecurity stakeholders in formulating and developing cybersecurity policies in each agency. This national cybersecurity strategy is prepared in line with the basic principles of national and state life, such as sovereignty, independence, security, togetherness, and adaptability.

Previous research by (Rahmawati, 2017) concluded that risk management in the field of information and communication, especially those related to citizens' lives or confidential data, is very important to reduce vulnerability to misuse of information and data in cyberspace. Risk management is considered a fundamental component of an effective strategy. Risk itself is a combination of the possibility of an event (likelihood) and the adverse effects of the event (consequence). Thus, risk management becomes crucial in preparing a strong national defense system.

Another study by (Nurain, Gultom, & Indrajit, 2024) suggests that attack identification can be done using the NIST framework consisting of seven incident recovery stages. This approach provides a solid foundation for understanding and addressing cyber risks in Internet of Things (IoT) and Cyber-Physical Systems (CPS) environments. The use of an integrated cybersecurity risk management framework for CPS, with reference to NIST guidelines, is considered essential to maintaining the security of critical infrastructure. This step allows systematic risk analysis and effective risk control so that business continuity can be guaranteed. Every critical infrastructure must run risk management processes efficiently to protect stakeholders' interests from potential financial, organizational, and reputational losses that could arise.

Based on the background description of the problem, researchers are interested in conducting research entitled "Development of Risk Management Systems to Reduce the Impact of Cyberthreats". This research can make a theoretical contribution to the development of risk management theory, especially in terms of cyber threats. Research findings can fill knowledge gaps and enrich literature related to risk management in facing information security challenges. The purpose of this study is to determine the effectiveness of risk management systems that can help organizations in reducing the impact of cyber threats.

Research Methods

This study used qualitative research methods. The qualitative research method is a way to examine a problem more deeply and thoroughly, which takes longer to complete (Kusumastuti & Khoiron, 2019). The data collection technique in this study is by literature study. Literature study data collection techniques involve a series of activities

related to library data collection methods, reading, recording, and managing research materials. This technique is carried out with the aim of revealing various theories that are relevant to the problem being studied (Darmalaksana, 2020). The data that has been collected is then analyzed in three stages, namely data reduction, data presentation and conclusions.

Results and Discussion

The 21st century is known as a digital era that provides convenience to all people, especially thanks to the use of the internet which contributes significantly in various sectors of life (Fonna, 2019). This changing era creates a trend where technology becomes an inseparable part of everyday life. This includes various aspects such as communication, online transactions, shopping, education, economy, health services, and various other needs that can now be easily done through the internet.

The convenience provided through the internet has provided significant benefits for all levels of society, especially in terms of accessing the flow of information. Quick access to information in different parts of the world is no longer limited to traditional mass media such as newspapers, radio, or television. Conversely, the existence of digital information such as that available through the internet has provided more opportunities for individuals to access information quickly. Thus, obstacles in the form of territorial boundaries become things that can be overcome easily (Prabowo, Wibawa, & Azmi, 2020). The presence of the internet also creates cyberspace, an area where communication occurs through computer networks, allowing everyone to connect with each other without the need to meet face to face. This cyberspace concept shows that in an online environment that uses computer network technology, individuals can access it as long as they have access to the network without the need to meet directly (Hertianto, 2021).

According to Heffter & Goel (2018), the development of modern technology driven by cyber innovation, has affected all aspects of life. The impact has made governments, individuals, and businesses highly dependent on the digital environment to carry out their daily activities (Hamonangan & Assegaff, 2020). However, at the same time there are opportunities for cybercrime such as cyber threats. A cyber threat is something that has not yet happened but has the potential to be able to do harm in this context both the tools used and the threat posed not physically but cyber. The definition of cyber threats can be interpreted as the tools used using information technology and computers and the losses caused also through information technology (Putri, Aditya, Musthofa, & Widodo, 2022).

In today's digital age, cyber threats continue to increase not only in some countries but almost all over the world. Cyberthreats include criminal acts that damage, manipulate, and steal important information from applications or websites, resulting in serious problems with the security of networks, databases, or computer systems (Parulian, Pratiwi, & Cahya Yustina, 2021). The following types of cybercrime attacks are cited in the study (Laksana & Mulyani, 2024), such as:

1. Phishing

These attacks are carried out by tricking victims into providing personal and confidential information, such as passwords or credit card numbers, through fake web pages or fake emails. Phishing attackers often use sophisticated social engineering methods to disguise the authenticity of websites or emails, making it difficult for victims to distinguish between fake and genuine sites. Even in organizations, this kind of attack can compromise the security of company information, cause sensitive data leaks, and

open opportunities for perpetrators to gain unauthorized access to internal company systems.

2. Malware attacks

Represents a serious threat in cybercrime, where malware is malicious software designed to damage or take control over a vulnerable computer system. These attacks are generally carried out through unsafe links or attachments in emails or social media. When a user accesses the link or opens the attachment, malware can enter the system and cause damage, data theft, or take control of the system without permission.

3. DDoS (Distributed Denial of Service) attacks

The perpetrators will try to disrupt the system by sending huge amounts of internet traffic to the intended target. This causes the system to be unable to function normally or even not accessible at all. DDoS attacks can cost a company a significant amount of time, money, and resources, as efforts to overcome the impact of such attacks require considerable effort and investment in system recovery.

4. Other types of attacks

In addition to the above attacks, there are still various other types of cybercrime attacks such as ransomware, spoofing, man-in-the-middle, and many more. Despite different methods, all of these attacks serve the same goal: undermining the integrity, confidentiality, or availability of data.

These types of cybercrime can clearly cause harm to both individuals and the business world. In the business world, cyber threats can cause serious disruption to company systems. If not handled properly, the impact can be very significant for the continuity of the company. According to (Muharam & Budianto, 2022) in business, cyberattacks can cause large financial losses, loss of important data, as well as damaged company reputations. In addition, cyberattacks can disrupt business operations, cause disruptions in customer service, and undermine customer trust. This means that companies that are unable to address cyber threats risk long-term consequences, such as bankruptcy risk. Therefore, efforts to prevent and address cyber threats are important in an evolving and digitally connected business environment.

According to (Mahendra & Soewito, 2023), every organization, both government and private, needs to have strong risk management to reduce the potential for cyberattacks. That is, in other words, risk management can serve as a strategic tool to reduce the impact of cyber threats. Risk management is one of the important elements in running a company's business because the growing world of companies and the increasing complexity of company activities result in increasing the level of risk faced by the company. The main objective of risk management implementation is to protect the company against losses that may arise (Arifudin, Wahrudin, & Rusmana, 2020).

Risk management is an approach that is organized systematically and logically. This approach is used to guide, identify, monitor, define solutions, report risks, and manage the organization. The purpose of this risk management practice is to deal with risks that may arise in order to maintain the sustainability and stability of the organization (Sajjad, Kalista, Zidan, & Christian, 2020). Another opinion conveyed by (A. Alijoyo, Wijaya, & Jacob, 2020) in his book, states that company risk management is the main approach in managing and optimizing risk, which allows companies to determine the extent of uncertainty and risk acceptable to the organization. By involving all aspects of the company, enterprise risk management serves as a strategic analysis of risk across the organization, cutting across business units and departments, and considering end-to-end processes. In adopting a risk management approach, companies gain the ability to align

their risks and tolerances with business strategies by identifying events that can be exploited as opportunities, while managing their adverse impacts, and further developing action plans to manage them (A. Alijoyo & Norimarna, 2021).

The importance of risk management, as highlighted by (Saputra, Ambarwati, & Setiawan, 2020), states that every company must have or implement appropriate risk management so that the security of information assets can be protected and at least reduce the impact of risks that will occur on the company. This means that risk management can play a key role in protecting an organization's information assets. This process begins with identifying potential cyber threat risks that can affect the security of the company's critical data and information. After identifying these risks, the next step is to develop an effective action plan to manage them.

Protection of corporate information assets, such as customer data, financial information, and business secrets, should be a key focus in risk management because of the critical characteristics of such information and the significant impact if it falls into the hands of unauthorized parties or competitors. The existence of information security breaches can provide an unfair competitive advantage or harm the value of the company. In addition, it can threaten relations with investors and other related parties. Protection of business secrets becomes very important to maintain competitive advantage and competitiveness in the market. This reflects that risk management is a crucial approach to prevent negative impacts and protect information assets that are very valuable to the company.

Risk management not only plays a role in protecting an organization's information assets, but can also increase resilience to cyberattacks through the implementation of appropriate frameworks. The framework serves as a guide to direct organizations in cybersecurity activities and incorporates cybersecurity risks as an integral part of the overall management process. The implementation of this framework provides clear steps and stages in improving cybersecurity through cybersecurity risk analysis (Ashari, 2018).

Several frameworks that include standards and guidelines related to risk management, such as ACT 2004, AS/NZS 2004, Committee 2004, DGQ 2007, FAA 2007, HB 2004, IEC 2008, ON 2008, Rio Tinto 2007, and Treasury Board of Canada 2001, can be used as a foundation for the organization (Pradana & Rikumahu, 2014). Understanding and managing risk through a framework is the process of helping an organization achieve its goals. The framework provides structure and guidance to assist organizations in identifying, assessing, and controlling risk. Through understanding and proactively managing risks using the framework, companies can achieve several positive results, such as firstly the implementation of this framework helps companies to be better prepared and responsive to cyber threats, secondly companies can implement specific and effective mitigation measures to minimize the possible impact of cyber threats, thirdly companies can maintain the continuity of their operations without disruption cyber threats.

Companies that successfully protect information assets and increase resilience to cyberattacks will have a positive impact in building customer trust. This signifies the company's dedication to maintaining data security and privacy, reflecting their seriousness towards ethical business practices. Data security is one of the main factors considered by customers when choosing a product or service. Companies that are known to have high security standards will gain greater trust from customers (Yunita, Sumarsono, & Farida, 2019). This trust becomes a solid foundation for forming long-term relationships, where customers feel comfortable sharing information with the company

and are confident that their privacy is respected. Through measures to protect information assets and increase resilience to cyberattacks, the company not only keeps customer data secure, but also builds a strong foundation for customer trust, a positive reputation, and support from various stakeholders.

Once the risks are identified and managed, the final stage involves an evaluation of risk management. Evaluation is a crucial step because the success of a program can be measured through the achievement of its objectives, showing that the components of the program are running well according to their functions. Evaluation is necessary to assess the extent to which the program achieves its objectives and the extent to which the components of the program perform their functions effectively. According to (Franciskus Antonius Alijoyo & Munawar, 2019), the application of risk management in organizations must continue to be developed and evaluated for the effectiveness of its application. To evaluate and assess the level of effectiveness of the implementation of organizational risk management, organizations can use a maturity measurement mechanism for the implementation of risk management. High maturity achievement is often described as a condition that indicates that risk management has been running effectively in the organization.

The evaluation section is important to ensure that the implementation of risk management is in accordance with the planning that has been done. The results of supervision and review can also be used as consideration for making improvements to risk management. Thus, an effective risk management system enables organizations to respond quickly and appropriately to emerging cyber threats. This helps maintain the smooth operation of the organization and provides maximum protection of sensitive information. The implementation of an effective risk management system is becoming a must for organizations facing increasingly complex and diverse cybersecurity challenges. In this way, organizations can be better prepared and able to respond to changes in a dynamic cyber environment.

Conclusion

The development of an effective risk management system is a crucial step for organizations in reducing the impact of cyber threats. A good risk management system plays an important role in protecting an organization's information assets, increasing resilience to cyberattacks, and building customer trust. By identifying, evaluating, and managing risks associated with information security, organizations can implement appropriate measures to minimize losses that may arise from cyberattacks. In addition, an effective risk management system also enables organizations to respond quickly and appropriately to emerging cyber threats, thus keeping organizational operations running smoothly and providing maximum protection of sensitive information. Thus, the implementation of an effective risk management system is a must for organizations in facing increasingly complex and diverse cybersecurity challenges.

References

Abdullah, Muhammad Subhan, & Ikasari, Ines Heidiani. (2023). Perkembangan Terbaru Dalam Keamanan Siber, Ancaman Yang Diidentifikasi Dan Upaya Pencegahan. *JRIIN: Jurnal Riset Informatika dan Inovasi*, *1*(1), 96–98.

Alijoyo, A., & Norimarna, Stefiany. (2021). The role of enterprise risk management (ERM) using ISO 31000 for the competitiveness of a company that adopts the value chain (VC) model and life cycle cost (LCC) approach. *3rd International Conference on Business, Management and Finance. Oxford, United Kingdom*, 11–14.

Alijoyo, A., Wijaya, Q. B., & Jacob, I. (2020). Failure Mode Effect Analysis Analisis Modus Kegagalan dan Dampak RISK EVALUATION RISK ANALYSIS: Consequences Probability Level of Risk. *Crms. www. lspmks. co. id*.

Alijoyo, Franciskus Antonius, & Munawar, Yusuf. (2019). Faktor yang mempengaruhi maturitas manajemen risiko organisasi di Indonesia. *Bina Ekonomi*, *23*(1), 67–79.

Arifudin, Opan, Wahrudin, Udin, & Rusmana, Fenny Damayanti. (2020). *Manajemen risiko*. Penerbit Widina.

Benyamin, Jefferson, Mualim, Much, & Duarte, Editha Praditya. (2023). Penilaian Keamanan Informasi Data Center Instansi Yaza untuk Mencegah Ancaman Siber dalam Meningkatkan Pertahanan. *Jurnal Ilmu Komputer dan Sistem Informasi (JIKOMSI)*, *6*(3), 180–190.

Darmalaksana, Wahyudin. (2020). Metode Penelitian Kualitatif Studi Pustaka dan Studi Lapangan. *Pre-Print Digital Library UIN Sunan Gunung Djati Bandung*.

Fonna, Nurdianita. (2019). Development of the Industrial Revolution 4.0 in Various Fields. *Bogor: Guepedia*.

Hamonangan, Iskandar, & Assegaff, Zainab. (2020). Cyber Diplomacy: Menuju Masyarakat Internasional yang Damai di Era Digital. *Padjadjaran Journal of International Relations*, *1*(3), 311–333.

Hertianto, M. R. (2021). Juridical Review of Child Protection in Cyberspace in Indonesia. *Journal of Law & Development*, *51*(3), 560.

Kusumastuti, Adhi, & Khoiron, Ahmad Mustamil. (2019). *Metode penelitian kualitatif*. Lembaga Pendidikan Sukarno Pressindo (LPSP).

Laksana, Tri Ginanjar, & Mulyani, Sri. (2024). Pengetahuan Dasar Identifikasi Dini Deteksi Serangan Kejahatan Siber Untuk Mencegah Pembobolan Data Perusahaan. *Jurnal Ilmiah Multidisiplin*, *3*(01), 109–122.

Mahendra, Vicky, & Soewito, Benfano. (2023). Penerapan Kerangka Kerja NIST Cybersecurity dan CIS Controls sebagai Manajemen Risiko Keamanan Siber. *Techno. Com*, *22*(3), 527–538.

Muharam, Novi, & Budianto, Azis. (2022). Carding Crime Analysis as A Form of Cyber Crime in Indonesia's Criminal Law. *Proceedings of the 2nd International Conference on Law, Social Science, Economics, and Education, ICLSSEE 2022, 16 April 2022, Semarang, Indonesia*.

Nurain, Amalia, Gultom, Rudy A. G., & Indrajit, Richardus Eko. (2024). Manajemen Ketahanan Risiko Siber pada Internet of Things dan Cyber Physical System. *Journal on Education*, *6*(2), 13271–13281.

Parulian, S., Pratiwi, D. A., & Cahya Yustina, M. (2021). *Ancaman dan Solusi Serangan Siber di Indonesia. Telecommunications, Networks, Electronics, and Computer Technologies (TELNECT), 1 (2), 85–92*.

Prabowo, Wisnu, Wibawa, Satriya, & Azmi, Fuad. (2020). Perlindungan Data Personal

Siber di Indonesia. *Padjadjaran Journal of International Relations*, *1*(3), 218–239.
Pradana, Yana Ayu, & Rikumahu, Brady. (2014). Penerapan Manajemen Risiko terhadap Perwujudan Good Corporate Governance pada Perusahaan Asuransi. *Trikonomika*, *13*(2), 195–204.
Putri, Amelia Widya Octa Kuncoro, Aditya, Abdul Razzaq Matthew, Musthofa, Desta Lesmana, & Widodo, Pujo. (2022). Serangan hacking tools sebagai ancaman siber dalam sistem pertahanan negara (studi kasus: predator). *Global Political Studies Journal*, *6*(1), 35–46.
Rahmawati, Ineu. (2017). Analisis Manajemen Risiko Ancaman Kejahatan Siber (Cyber Crime) dalam Peningkatan Cyber Defense. *Jurnal Pertahanan dan Bela Negara*, *7*(2), 35–50.
Sajjad, Mudrika Berliana As, Kalista, Salsabila Dea, Zidan, Mualif, & Christian, Johan. (2020). Analisis manajemen risiko bisnis. *Jurnal Akuntansi Universitas Jember*, *18*(1), 51–61.
Saputra, Rizky Ramadhan, Ambarwati, Awalludiyah, & Setiawan, Eman. (2020). Manajemen Risiko Teknologi Informasi Menggunakan Octave Allegro Pada Pt. Hd. *SITEKIN: Jurnal Sains, Teknologi Dan Industri*, *17*(1), 1–10.
Sudarmadi, Damar Apri, & Runturambi, Arthur Josias Simon. (2019). Strategi Badan Siber dan Sandi Negara (BSSN) Dalam Menghadapi Ancaman Siber di Indonesia. *Jurnal Kajian Stratejik Ketahanan Nasional*, *2*(2), 157–178.
Yunita, Nahla Rahma, Sumarsono, Hadi, & Farida, Umi. (2019). Pengaruh Persepsi Risiko, Kepercayaan, Dan Keamanan Terhadap Keputusan Pembelian Online Di Buka Lapak (Studi Kasus Pada Komunitas Buka Lapak Ponorogo). *ISOQUANT: Jurnal Ekonomi, Manajemen Dan Akuntansi*, *3*(1), 90–105.